# C4I Interoperability Certification & Testing Process

# Overview

- Definitions
- Interoperability Policy & Guidance
- Interoperability Certification Process
- Interoperability Testing Process
- Observations & Challenges
- Joint Interoperability Test Command (JITC) Information
- DoD IT Standards Registry (DISR)
  - Formerly called Joint Technical Architecture (JTA)
- Joint Tactical Radio System (JTRS)

# Definitions

# What is Interoperability?

**“Ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.”***

***(JCS Pub 1)***

# System-of-Systems

## CJCSI 3170.01D

**System-of-Systems.**

A set or arrangement of interdependent systems that are related or connected, to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole.

**Key Points**

- Arrangement of systems
- Related or connected systems
- Provide a given capability

**One Function Concept**

- Loss of part
- Degrades the whole

**Limited Redundancy**

# System-of-Systems Military

Provide a given Functional Capability…

| System | of Systems |
| --- | --- |
| Comanche Helicopter | propulsion, navigation, targeting, weapons, FBCB2 |
| Abrams Tank | propulsion, navigation, targeting, weapons, FBCB2 |
| Paladin Howitzer | propulsion, navigation, targeting, FBCB2 |

# *Family-of-Systems*

**CJCSI 3170.01D**

**Family-of-Systems.**

A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capability needs. The mix of systems can be tailored to provide desired capabilities, dependent on the situation.

## Key Points

- Independent systems
- Arranged or interconnected
- In different ways
- Different capabilities

**Multiple Function Concept**

- Flexible mix
- To provide capabilities
- For situation

**Flexible Capabilities**

# Family-of-Systems Military Ex

**Capability:** Gather process and disseminate information in five functional areas—Maneuver Control, Intelligence, Artillery, Air Defense, and Logistics.

**Family of Systems:**

MCS Maneuver Control

ASAS Intelligence

ATCCS AFATDS Artillery

AMDWS Air Defense

CSCSS Logistics

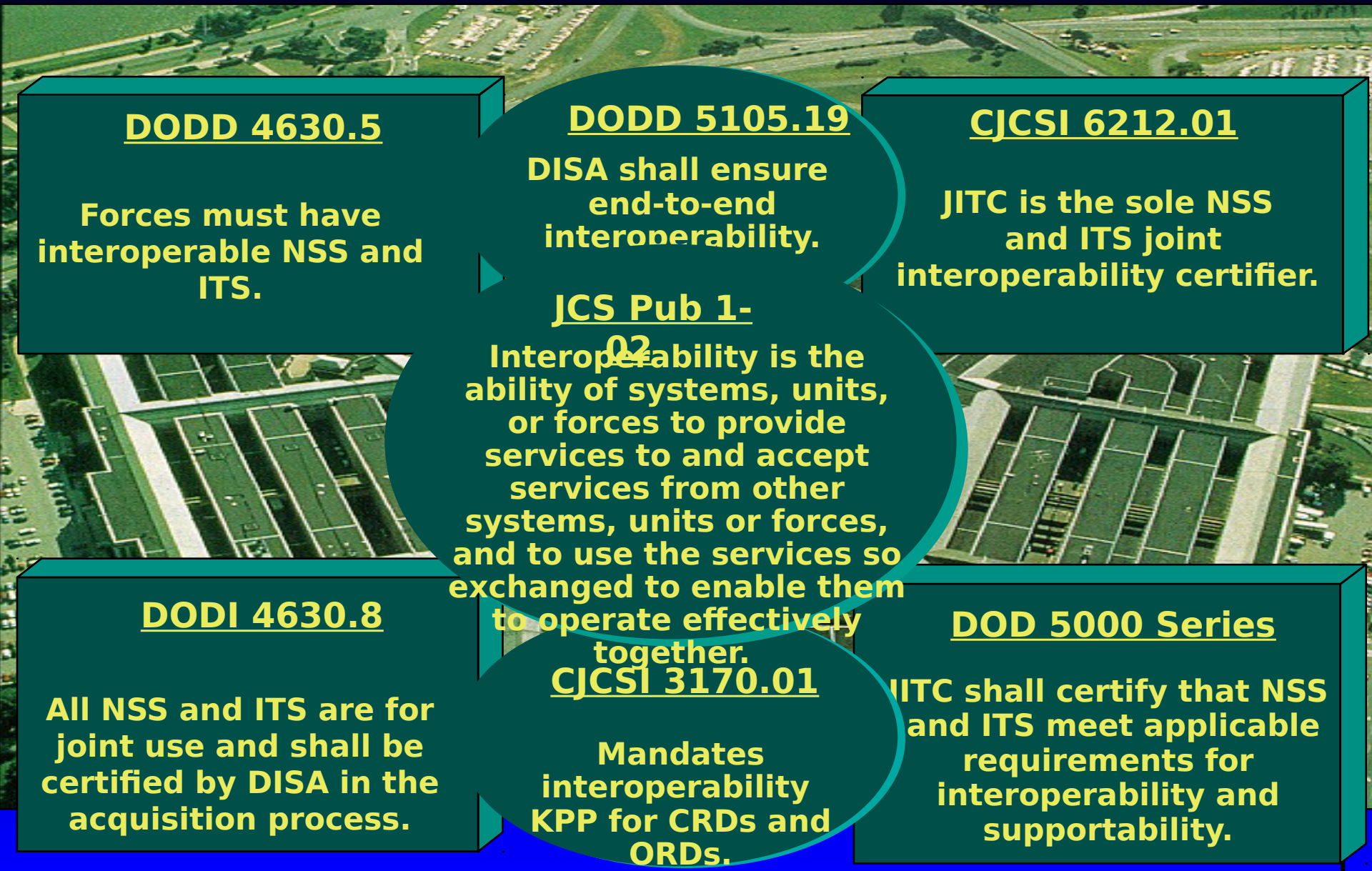
GCCS-A Component HQs

ABCS ATCCS Tactical Operations Centers

FBCB2 Platforms

# Interoperability Policy and Guidance

# JOINT INTEROPERABILITY DIRECTIVES



**DODD 4630.5**

Forces must have interoperable NSS and ITS.

**DODD 5105.19**

DISA shall ensure end-to-end interoperability.

**CJCSI 6212.01**

JITC is the sole NSS and ITS joint interoperability certifier.

**JCS Pub 1-02**

Interoperability is the ability of systems, units, or forces to provide services to and accept services from other systems, units or forces, and to use the services so exchanged to enable them to operate effectively together.

**DODI 4630.8**

All NSS and ITS are for joint use and shall be certified by DISA in the acquisition process.

**CJCSI 3170.01**

Mandates interoperability KPP for CRDs and ORDs.

**DOD 5000 Series**

JITC shall certify that NSS and ITS meet applicable requirements for interoperability and supportability.

# Good Websites – Interoperability Info

- www.teao.saic.com/jfcom/ier/resources/resources.htm
  - Documents & reference material
  - Training
- JIST3 (TECNET) http://tecnet0.jcte.jcs.mil/
- AKSS or legacy Deskbook www.dau.mil

# SoS and FoS Interoperability

**DoD Directive 5000.1: Defense Acquisition Process**

**Systems, units and forces shall be able to provide and accept data, information, materiel, and services to and from other systems, units and forces; and shall effectively interoperate with other U.S. Forces and coalition partners. Joint concepts and integrated architectures shall be used to characterize these interrelationships.**

**DoD Instruction 5000.2: Operation of the Defense Acquisition System**

- **Requires interoperability requirements in a family-of-systems mission area context**
- **Interoperability certification prior to Full Rate Production Decision Review**

# The Net-Centric Checklist

**The Net-Centric Checklist will be included in the new DoD 5000 "Guidebook"**

- **Checklist's purpose is to assist PMs in understanding the Net-Centric attributes their programs need to implement**
- **Four sections to checklist: Data, Services, IA / Security, Transport**
- **OSD may use checklist during program reviews, and / or as part of the annual budget request process**
- **Checklist is available from DoD Chief Information Officer**

# Key Performance Parameters

- Prior to Nov 03, all systems with top-level information exchange requirements, an interoperability KPP was required
- Capabilities documents submitted Nov 03 to May 04, interoperability KPP with migration strategy to Net Ready KPP
- All JCIDS capabilities documents submitted after May 04, will include the NR-KPP, unless JROC grants exemption for a specific program
  - Legacy Requirements Generation System documents will continue to contain the interoperability KPP
  - Validated and approved ORDs may be used to support MS B or MS C decisions until 24 June 2005

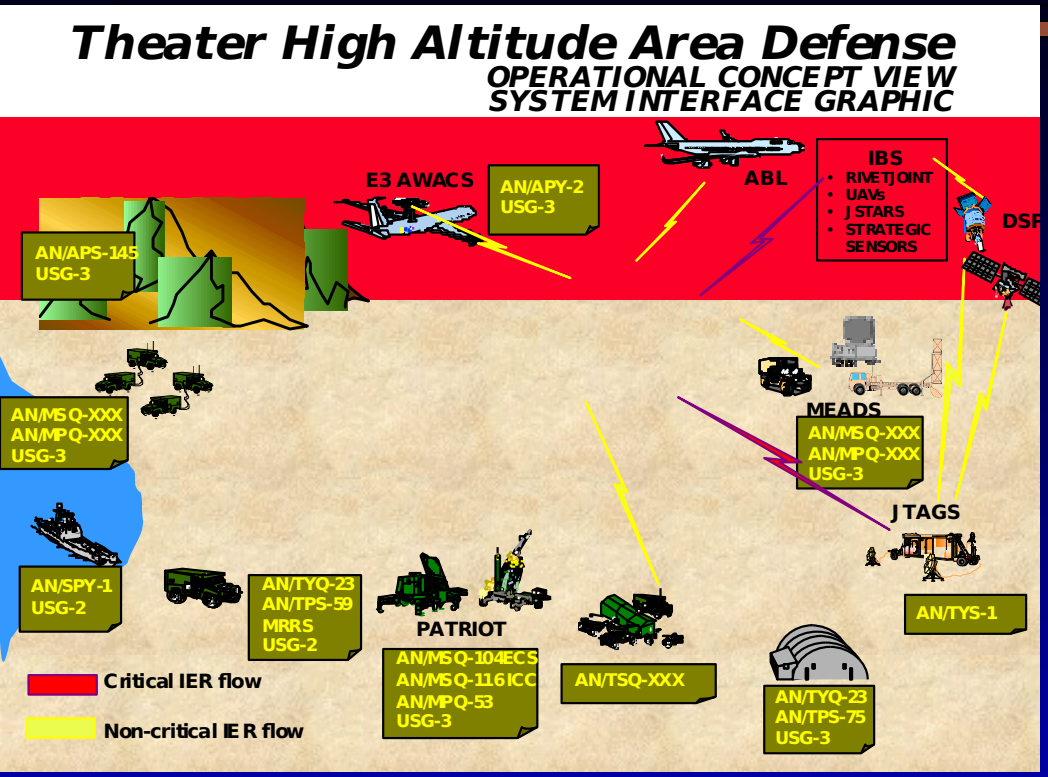
# Interoperability KPP

- Legacy requirements documents required to include interoperability key performance parameters (KPPs) and information exchange requirements (IERs)
  - Mandatory, regardless of ACAT
  - Interoperability KPP is derived from the top-level IERs
  - Interoperability will be a KPP in every increment of a spiral development program (if there are top-level IERs)

# What is an IER?

- Information Exchange Requirement – the requirement for information to be passed between & among forces, organizations, or administrative structures, concerning on-going activities
- An IER tells you:
  - Who is sending the information
  - What information is being sent
  - Why the information is being sent
  - Who is receiving the information
  - How the information must be passes, for the mission / process / transaction to be successfully completed

# Example: ORD Interoperability




UNCLASSIFIED

## Theater High Altitude Area Defense
### Top-Level IER Matrix Extract

| Event | Info Category | Sending Node | Receiving Node | Priority | Critical | Format | Timeliness | Freq | Class | Size | Remarks |
|---|---|---|---|---|---|---|---|---|---|---|---|
| TBM Launch & Detection | Targeting | IBS, CRC/ACC, ABL, JSTARS, PAC-3 | THAAD | OP225, OP242, OP616 | Y | Data (TADIL), Voice | <2 Sec | Event Driven | S | 128 bits 3 Sec | Set up and detection to support attack operations. Early warning. Status THAAD Unit/System. Info to THAAD support and engagement. Launch EEI. |
| Provide ROE Update | Situational Awareness | CRC/ACC, PAC-3, NAOC, NCA/CS | THAAD | OP532, OP543 | N | Data (SMTP) | <2 hrs | 2/Day | S | <400 Characters | Set to provide ROE to JTAN required. Shall serve THAAD sensors |
| Collect Target Information | Situational Awareness | IBS, CRC/ACC, ABL, JSTARS, PAC-3 | THAAD | OP224 | Y | Data (TADIL) | <2 Sec | Event Driven | S | 128 bits | Acquire information that supports detection, identification, and location of enemy targets with ABL and |
| Collect Target Information | Situational Awareness | ABL, NAOC | THAAD | OP224 | N | Data (TADIL) | <2 Sec | Event Driven | S | 128 bits | Acquire information that supports detection, identification, and location of enemy targets with ABL and |
| Attack Operations Tasks | Targeting | THAAD | CRC/ACC, IBS | OP32 | N | Data (TADIL) | <2 Sec | Event Driven | S | 128 bits | Tactical information, location of target, attack guidance, execution |
| Synchronize Operational Response | Targeting | IBS, CRC/ACC, ABL, JSTARS, PAC-3 | THAAD | OP327 | Y | Data (TADIL) | <2 Sec | Event Driven | S | 128 bits | Enemy attacks, friendly forces, results of attacks, destruction, future engagements, track data, KA/LOW track, course, track speed, track altitude, |

## Interoperability KPP

| | Threshold (T) | Objective (O) |
|---|---|---|
| **All IERs will be satisfied to the standards specified in the T and O values.** | **100% of IERS designated critical** | **100% of IERS** |

# Example: ORD Interoperability KPP

UNCLASSIFIED

## Theater High Altitude Area Defense
### Top-Level IER Matrix Extract

| Event | Info Characteristics | Sending Node | Receiving Node | Related OPs | Critical | Format | Timeliness | Freq | Class | Size | Remarks |
|---|---|---|---|---|---|---|---|---|---|---|---|
| TBM Launch & Detection | Targeting | BFTN, CRC/ACC, AEGIS, JTAGS, PATRIOT | THAAD | OP2.2.5, OP2.4.3.4, OP2.4.2.2, OP6.1.6 | Y | Data (TADIL), Voice | <12 Sec | Event Driven | S | 32 bits / 30 sec | Set up and direct tests to support attack operations. Both voice & TADIL-J from THAAD to support ongoing Joint OPLAN. |
| Provide ROE Update | Situational Awareness | CRC/ACC, PATRIOT, NTACS | THAAD | OP5.3.2, OP5.4.3 | N | Data (USMTF) | <2 Hrs | 2/Day | S | <6000 Characters | Set to provide ROE to THAAD as required. Both voice & TADIL-J in THAAD unit. |
| Collect Target Information | Situational Awareness | BFTN, CRC/ACC, AEGIS, JTAGS, PATRIOT | THAAD | OP2.2.4 | Y | Data (TADIL) | <12 Sec | Event Driven | S | 32 bits | Acquire information that supports detection, identification, and location of enemy targets with AB and NTACS. Both voice & TADIL-J. |
| Collect Target Information | Situational Awareness | AB, NTACS | THAAD | OP2.2.4 | N | Data (TADIL) | <12 Sec | Event Driven | S | 32 bits | Acquire information that supports detection, identification, and location of enemy targets with AB and NTACS. Both voice & TADIL-J. |
| Attack Operations Targets | Targeting | THAAD | CRC/ACC, BFTN | OP3.2 | N | Data (TADIL) | <12 Sec | Event Driven | S | 32 bits | Target identification, and location, target track updates to support both attack operations. Both voice & TADIL-J. |
| Synchronize Operational Fires over | Targeting | BFTN, CRC/ACC, AEGIS, JTAGS, PATRIOT | THAAD | OP3.2.7 | Y | Data (TADIL) | <12 Sec | Event Driven | S | 32 bits | Enemy tracks, friendly forces, restricted areas, no-fire areas, identification required, clearing fires, track data, track quality, track course, track speed, track altitude, engagement status. Both voice & TADIL-J. |

# Net-Ready KPP

- The NR-KPP is used to assess:
  - Information needs
  - Information timeliness
  - Information assurance
  - Joint interoperability and supportability
  - Attributes required for technical exchange of information, and end-to-end effectiveness of the exchange
- The NR-KPP consists of measurable, testable, or calculable characteristics and performance metrics
  - The NR-KPP Key Interface Profiles (KIPs) are currently under development. Programs must incorporate applicable KIPs, as they become available.
  - See CJCSI 6212.01series for more information

| Net-Ready KPP | Threshold (T) | Objective (O) |
| --- | --- | --- |
| All activity interfaces, services, policy-enforcement controls, and data-sharing of the NCOW-RM and GIG-KIPs will be satisfied to the requirements of the specific Joint integrated architecture products (including data correctness, data availability and data processing*), and information assurance accreditation, specified in the threshold (T) and objective (O) values. | 100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements designated as enterprise-level or critical in the Joint integrated architecture**. | 100 percent of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements in the Joint integrated architecture. |

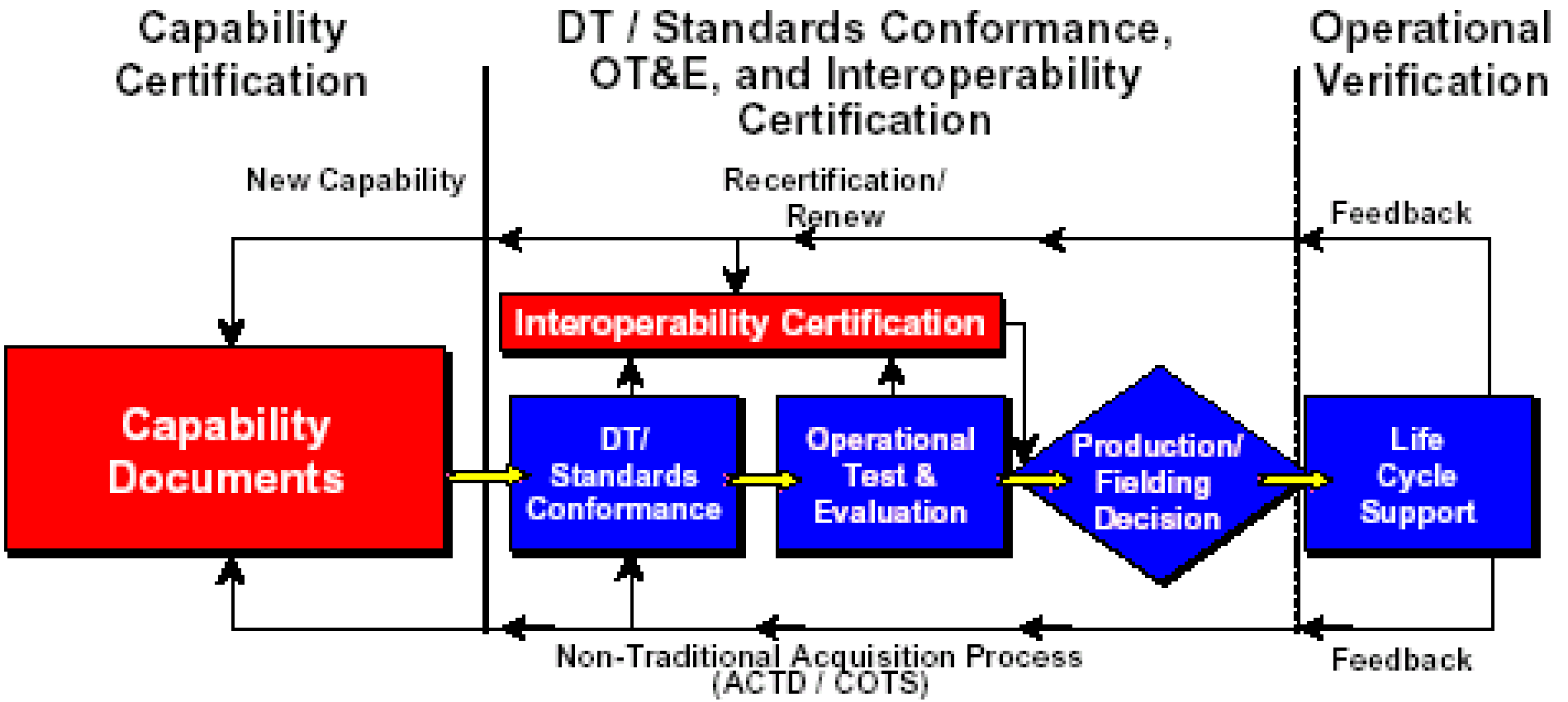
# Interoperability (Net-Ready) Certification Process

# Three Types of Certification / Validation

**Applies to all ACATS, non-ACATs, & all fielded systems**

1. J-6 Capabilities Interoperability Certification
   - Occurs prior to each milestone
   - J-6 certifies capabilities documents and NR-KPPs for conformance with joint NSS and ITS policy and doctrine and interoperability standards.
2. Supportability Certification – J-6 certifies that programs adequately address infrastructure requirements, availability of bandwidth, spectrum support, and identify deficiencies and interface requirements between systems
3. Interoperability System Validation – J-6 validates that the NR-KPP was adequately tested during the DISA (JITC) interoperability test certification (Net-Ready certification).

# JITC Testing Process
## Life-Cycle Certification Process



# Interoperability / Net-Ready Certification Process

- The Certification Team (including the system proponent, system developer, user rep., and JITC) work together to:
  - Identify & verify joint interoperability requirements
    - Identify all systems that need to be interfaced
    - Determine requirements criticality
  - Determine the scope & extent of testing, and perform interoperability / Net-Ready testing
  - Determine whether interoperability / Net-Ready requirements are met for joint use

# What Systems Need Interop. Certification?

- All Command, Control, Communications, Computers, and Intelligence (C4I) and Automated Information Systems (AIS) that:
  - Are developed for use by US forces (National Security Systems)
  - Produce, use or exchange information in any form
  - Exchange information between Services, agencies, or countries
  - Must operate within a joint interface
  - Includes weapon systems with C4I subsystems
  - Includes all ACAT, non-ACAT, and fielded systems

# Interoperability / Net-Ready Test Certification

- Certification is required, prior to Full Rate Production DR
- Fielded systems must be recertified after a major modification, or every three years. (This includes legacy systems.)
- Director, DISA certifies to the appropriate DT and OT organizations and to the Chairman JCS (based on JITC recommendation)
- JS (J-6) validates that the interoperability NR-KPP was adequately tested during the DISA (JITC) interoperability test certification (Net-Ready certification).
- Failure to meet certification may be interpreted that a system is not operationally effective (NR-KPP)

# Failure to Meet Certifications

- If a program / system fails to meet certification requirements, the J-6 will:
  - Not validate the program
  - Recommend the program not proceed to the next milestone
  - Recommend that funding be witheld until compliance is achieved and the program / system is validated
  - Request the program / system be added to the DODI 4630.8 Interoperability Watch List

# Interoperability “Watch List”

- Programs with significant interoperability deficiencies may be put on “Watch List” (JCS, OSD)
- PM must take corrective action & report progress to ASD(C3I), USD(AT&L), JS, DOT&E
- If deficiencies persist, program or system may be proposed for T&E Oversight

# To Get & Keep Your System Certified:

- The system proponent should contact JITC early in the acquisition program, to ensure that certification is both timely and cost-effective
- Coordinate all testing with JITC, so joint interoperability testing can be integrated into the test program schedule
- Consult JITC on changes in requirements or capabilities, in order to keep certification status current

# Interoperability Testing Process

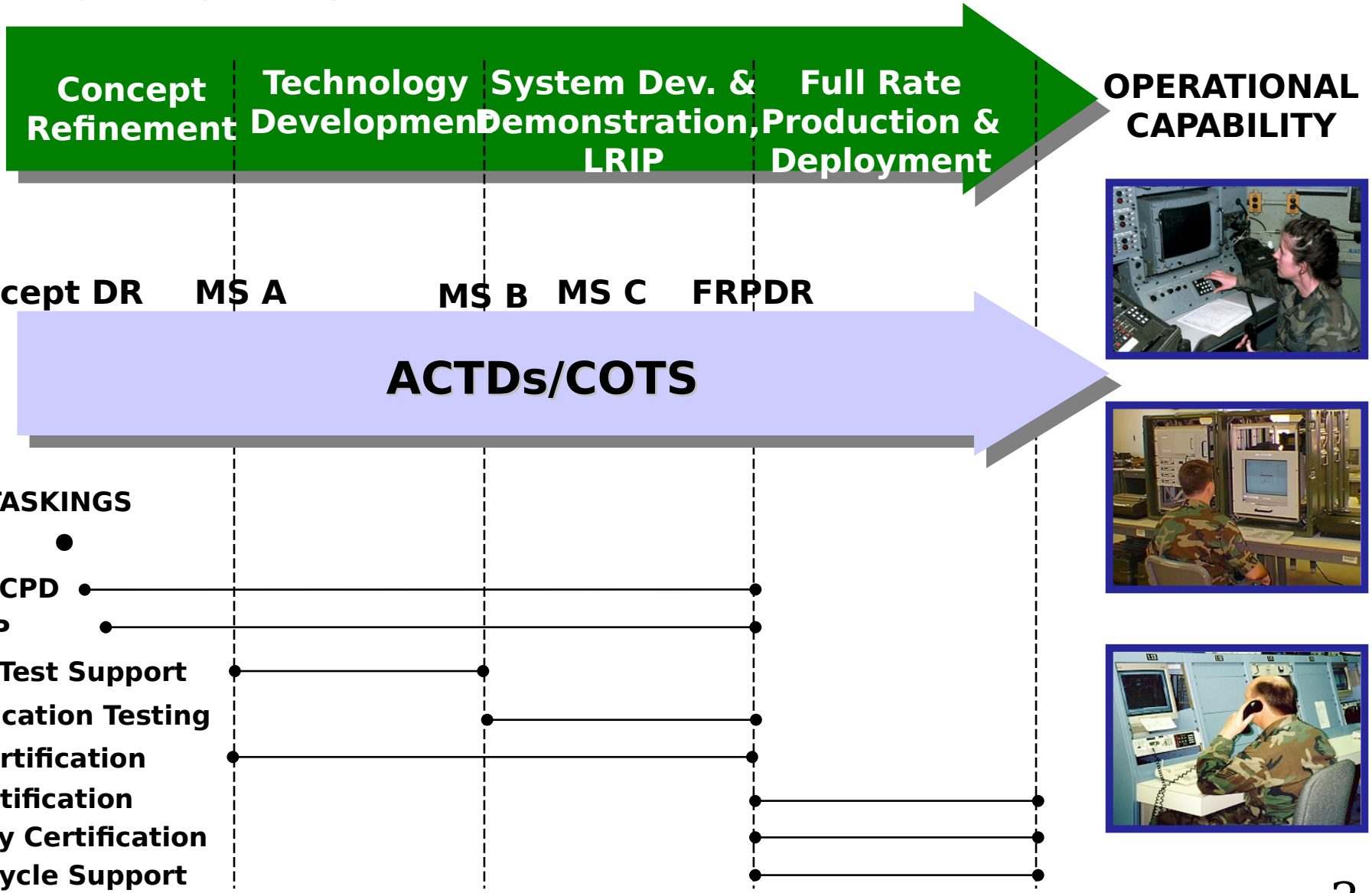
# Interoperability Testing

- JITC definition - Interoperability testing is the process of assessing the system's ability to exchange usable electronic information with systems of other services or nations, as specified in the requirements documents.
  - Specialized test tools are used to monitor performance (to determine if the proper actions and reactions are produced)
  - A system is certified as interoperable at the completion of successful interoperability testing.
- Note: JITC is not the only test agency looking at interoperability.
  - DT&E, DOT&E, and OTAs assess interoperability as part of the T&E process.

# JITC Test Process

- JITC review & analysis of system requirements, test plans (including TEMP), and test results.
- If testing is conducted by JITC – JITC performs test planning, execution & reporting activities (cost-reimbursable basis).
- Testing may be conducted by JITC or another test agency
  - JITC must approve that agency's test plans prior to start of testing
  - For certification decisions - JITC will review any available interoperability / Net-Ready test data – JITC can use test results from other test facilities to provide info for joint certification requirements (JITC typically must witness interoperability testing done by other organizations).
  - JITC review / analyze / assess test results from all sources

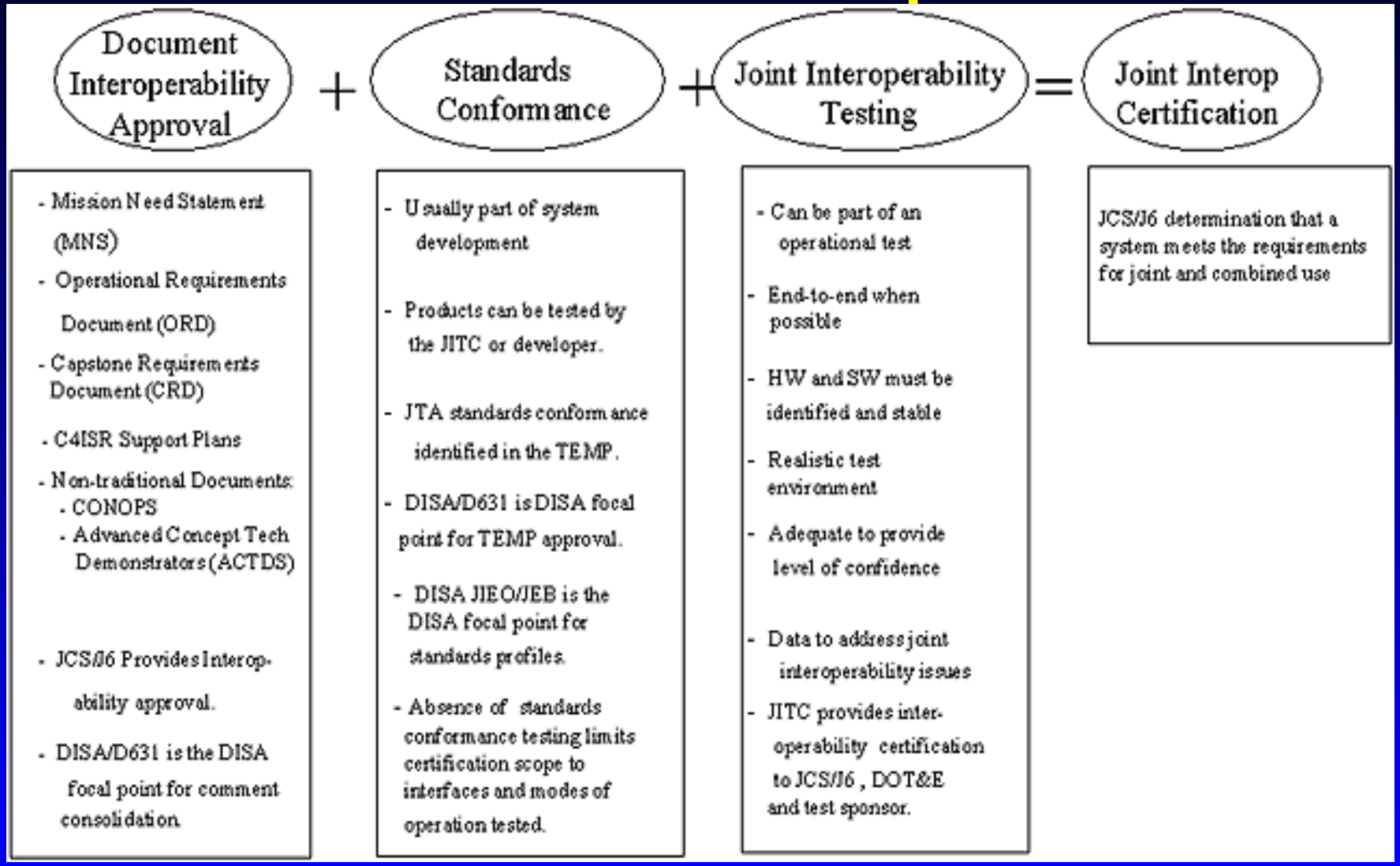
# Acquisition Process - JITC Involvement



# Interoperability KPP Scope of Testing

- Interoperability Testing
  - Can we send information from one system to another
  - Test interoperability between the various systems
- Standards Conformance Testing
  - Can the system use information received from another system
  - Tests system conformance with applicable standards

# Interoperability KPP Certification Components


Document Interoperability Approval
+
Standards Conformance
+
Joint Interoperability Testing
=
Joint Interop Certification
- Mission Need Statement (MNS)
- Operational Requirements Document (ORD)
- Capstone Requirements Document (CRD)
- C4ISR Support Plans
- Non-traditional Documents:
- CONOPS
- Advanced Concept Tech Demonstrators (ACTDS)
- JCS/J6 Provides Interop-ability approval.
- DISA/D631 is the DISA focal point for comment consolidation.
- Usually part of system development
- Products can be tested by the JITC or developer.
- JTA standards conformance identified in the TEMP.
- DISA/D631 is DISA focal point for TEMP approval.
- DISA JIEO/JEB is the DISA focal point for standards profiles.
- Absence of standards conformance testing limits certification scope to interfaces and modes of operation tested.
- Can be part of an operational test
- End-to-end when possible
- HW and SW must be identified and stable
- Realistic test environment
- Adequate to provide level of confidence
- Data to address joint interoperability issues
- JITC provides inter-operability certification to JCS/J6 , DOT&E and test sponsor.
JCS/J6 determination that a system meets the requirements for joint and combined use

# Net-Ready KPP Scope of Testing

- Information Needs
  - Precepts
  - Nodes, Needlines and Activities
  - Organizational Relationships
  - Systems Information Exchanges
  - Activities & Process Flows
  - Data Flows
  - Capability to System Trace
- Information Timeliness
  - Required Systems Information Exchanges
  - Performance Attributes – Periodicity, Timeliness, Availability, Throughput
  - Time Ordered Nodal Information Exchanges
  - Capability to Systems Correlation to Meet Timeliness Requirements

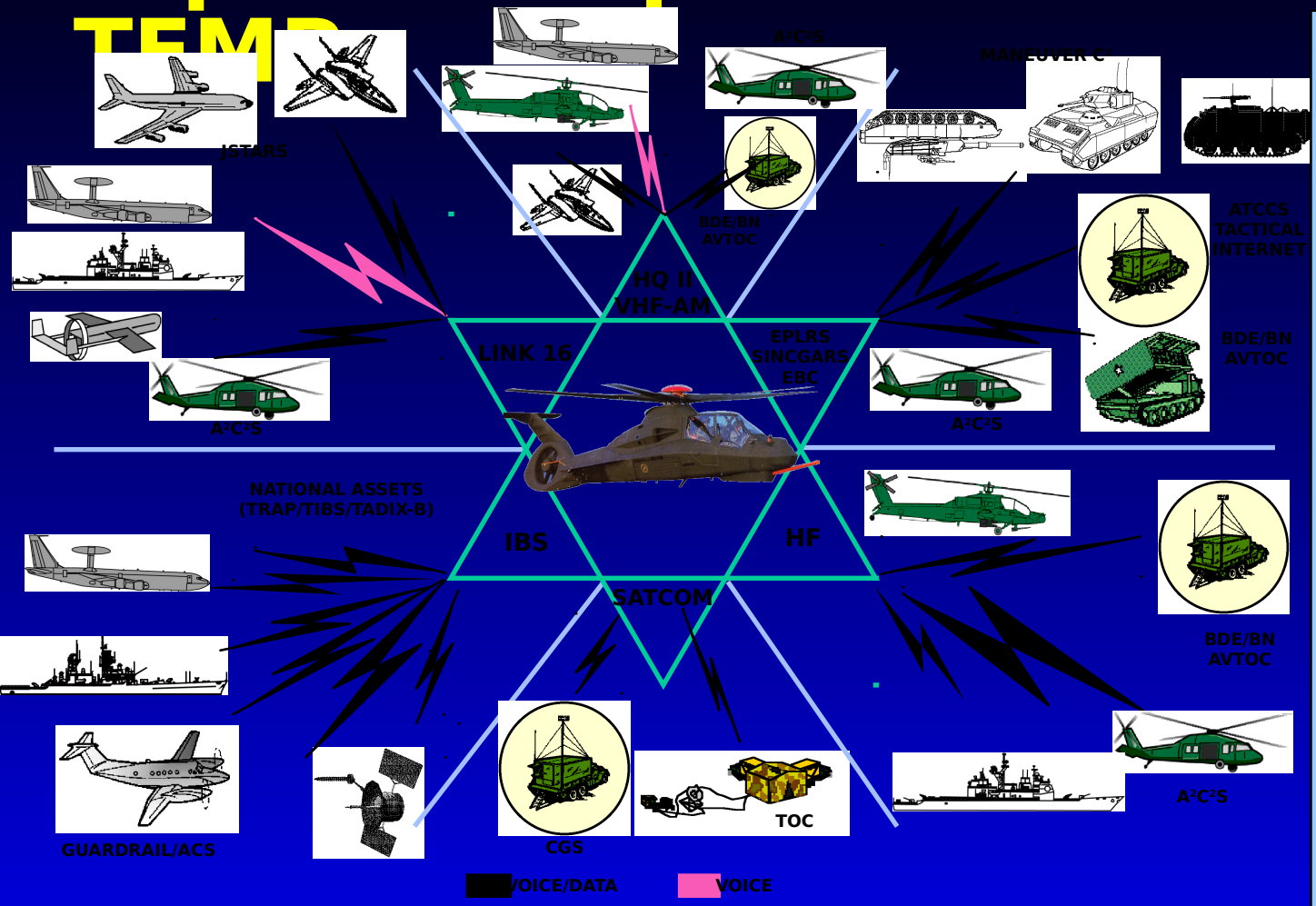
# Net-Ready KPP Scope of Testing

- Information Assurance
  - Required Systems Information Exchanges
  - Performance Attributes – Accuracy, Information Criticality, Availability, Integrity
  - Data Flows / Formats
  - Information Sequencing
  - Capability to Systems Correlation to Meet Information Assurance Requirements
- Net-Enabled
  - Node Connectivities and Information Needs
  - Capability to Systems Correlation
  - Mapping to NCOW Activities Model
  - Data Flows / Formats
  - Technical Standards Required to Implement Capability
  - Information Sequencing
  - SV-TV Bridge

# TEMP Considerations

- Part I: SYSTEM INTRODUCTION
  - System Description: interoperability with existing and /or planned systems of US or allies;operational and system architecture views
  - At least one critical issue and critical technical parameter for interoperability is required
- Part II: INTEGRATED TEST PROGRAM SUMMARY
  - Interoperability roles and responsibilities on T&E IPT. Schedule
- Part III: DEVELOPMENTAL TEST AND EVALUATION OUTLINE
  - Technical T&E of interoperability, incl. M&S (HWIL, SIL)
  - DT&E plans to support JITC/DISA interoperability certification recommendation to J-6
- Part IV: OPERATIONAL TEST AND EVALUATION OUTLINE
  - Operational T&E of interoperability, incl. JITC testing
  - Plans for interop. testing with other US and allied weapon systems
- Part V: TEST AND EVALUATION RESOURCE SUMMARY
  - Provide the resource requirements to support conduct of interoperability testing in DT and OT; identify shortfalls

# Example: Interop. Architecture Top Level Operational View for TEMP




***Connectivity via Voice and Data Links to:***

- ***Army Systems***
  - ***Maneuver CDR TOC (ATCCS) (Via EBC Using SINCGARS and EPLRS)***
  - ***AVTOC***
  - ***Apache Longbow***
  - ***A2C2S***
  - ***Bradley***
  - ***Crusader***
  - ***Abrams***
  - ***Land Warrior***
  - ***GUARDRAIL/ACS***
  - ***UAV Digital Data Link (TCS)***
- ***Joint/National Systems***
  - ***JSTARS (LINK 16)***
  - ***AWACS***
  - ***F-15, F-16, F-22, JSF***
  - ***F-18, AH-1W***
  - ***AEGIS Cruisers***
- ***Use of Standard Message Formats***
  - ***JVMF***
  - ***TADIL/J***

- **Common Aviation Embedded Battle Command (EBC) Solution**
- **Flexible Architecture/Software Configurable**
- **ITRS Compliant**

# Interoperability Observations and Challenges

# Interoperability Issues

- Most “stovepipe” legacy systems were not designed to share information outside their stovepipe
- Systems required / designed to share information does not fully achieve that objective. Many causes:
  - Low priority for joint and combined interoperability
  - Ambiguous/loose military standards (message formats, symbology, etc)
  - Incompatible technical approaches / data
  - Cultural / process obstacles (example: sharing classified information in coalition)
  - Poor synchronization across programs.
    - Upgrades applied in uncoordinated, stovepipe fashion
  - Lack system-of-systems engineering & integration (SE&I) function

# Top 10 - Interoperability Myths

1. This is not a joint program – interop doesn't apply
2. This is a stand-alone program – interop doesn't apply
3. This is just a system upgrade – interop doesn't apply
4. This is a combat weapons system – interop is for C2 systems
5. Interop is the responsibility of the common hardware, not the weapons system
6. If we apply the MILSTDs and DII-COE, we'll be interoperable
7. Interoperability T&E is an unfunded requirement (We can't pay the bill to test other systems interop with our system)
8. Soldiers take the system and make interop happen – it's all TTP
9. Interop is JITCs job; our job is performance
10. We passed interop certification; we're home free for all block upgrades!

# Interoperability Lessons Learned

- Make sure interoperability testing is a priority
- Interoperability testing must reflect real world situations and operational environments
- Interoperability Is a Key Risk Area Even When Developing Systems Using Commercial Off-the-shelf (COTS) Solutions.
  - Cost Drivers Implementing COTS in DoD S-o-S Environment Increase Overall IT Acquisition Costs From Ten to Fifteen Percent of Overall Acquisition Development Cost. (Interoperability is a key cost and schedule driver)
  - Costs Escalate Due to Difficulties Establishing Interface With Obsolescent Technology and Data Base Systems, Accommodating Classified or Sensitive Data, and Conjoining Incompatible Proprietary COTS Software Packages.

# Funding

- Funding is needed all phases and aspects of interoperability testing
  - Responsibility of PM for pre-Full Rate Production
  - For post-Full Rate Production, funding may be provided by JITC and / or PM
- Currently a lot of unfunded interoperability requirements
- PM must plan and budget for interoperability / Net-Ready certification and testing

# Recommendations

- **Adequately address interoperability NR-KPP testing in T&E planning**
  - Address cost
  - TEMP must include interoperability test strategy, certification plans, and required resources
- **Maintain stable requirements across all segments (within systems of systems) to foster "harmonious" development:**
  - Synchronize requirements and schedules for All segments.
  - Clearly lay-out block upgrade requirements.
  - Requirements should be firm upon contract award – **modify only along with concerted spiral development efforts**

# Recommendations (Cont.)

- Ensure compliance with interoperability standards
- Develop appropriate technical interoperability metrics (message completion rate, speed of service, etc.)
- High level of management attention for systems of systems
- Change the “traditional approach” of focusing on each system in isolation
  - Joint interoperability is just as important as intra-Service interoperability

# Joint Interoperability Test Command (JITC) Information

# JITC Website

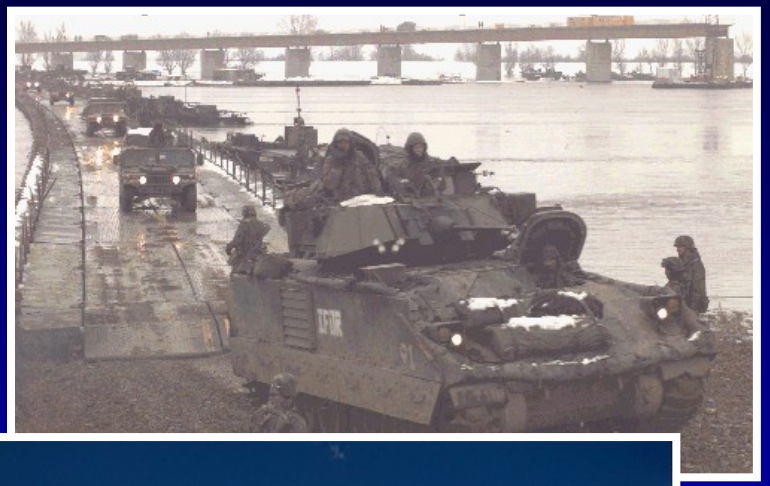
- Joint Interoperability Test Command (JITC)
  - http://jitc.fhu.disa.mil
  - 1-800-let-jitc
  - (520) 538-5482

# JITC Operational Test Agency

- **DISA Programs**
  - **Global Command and Control System**
  - **Defense Message System**
  - **Defense Information System Network**
- **DLA Programs**
  - **Distribution Standard System**
  - **Environmental Reporting Logistics System**
  - **Fuels Automated System**
  - **Defense Reutilization and Marketing Service Automated Information System Modernization**
  - **Standard Procurement**
- **SOCOM Programs**
  - **Special Operations Media System B**
- **OTHERS**
  - **Defense Commissary Agency**
  - **Defense Finance and Accounting Service**
  - **Air Force Space Command**

# JITC Mission Areas

- **Operational test and evaluation for Joint C4I systems**
  Operational Test Agency (OTA) for Joint Systems (GCCS, GCSS, DMS, DISN) and other DoD elements



- **DoD joint interoperability assessment and certification**
  Sole Joint C4I System Interoperability Certifier (DoDD 4630.5, DoDI 4630.8, CJCSI 6212.01A)

- **C4I technical assistance**

# JITC C4I Assistance to Warfighters

- **C4I systems and networks**
  - **Real world contingencies**
  - **Exercise support**
  - **Field assessments**
  - **On-site technical assistance**

# JITC Testing

- Criteria for measuring success
  - Requirements Documents
  - Test for success
  - Conduct certification testing for system characterization
  - Ensure operational capability
- Major inhibitors
  - Fast track acquisition process
  - Service vs. Joint acquisition
  - Distributed operational environment
  - Affordable confidence
- JITC's follow-on program
  - Validate and verify certifications
  - Capture systems that escaped acquisition cycle
  - Operate and maintain C4I equipment

# DoD Information Technology Standards Registry (DISR)

## DISR was Formerly Called Joint Technical Architecture (JTA)

# DoD IT Standards Registry (DISR)

- Provides the foundation for a seamless flow of information & interoperability among all tactical, strategic & combat support systems that produce, use or exchange information electronically.
- Mandates standards & guidelines for system development & **acquisition** that will dramatically reduce:
  - Cost
  - Development time
  - Fielding time for improved systems

# DISR Characteristics

- Contains standards applicable to all DoD systems that produce, use, or exchange information
- Standards are stable, technically mature, publicly available
- Contains mandatory & emerging standards
- Living document; evolving with technology & marketplace

# DISRonline

- DISRonline is the electronic version of DISR / JTA
  - DISRonline addresses all versions of JTA / DISR
- A system profile / IT standards profile(s) developed on DISRonline must be submitted to Joint Staff (J6) for all new & improved systems within DoD (CJCSI 6212C)
  - A system profile (ex: for a new airplane) contains IT profiles (for flight controls, avionics, navigation, etc.)

# IT Standards Profiles

- An IT profile is a list of standards (plus associated information), chosen from the list of available standards in that version of JTA or DISR
  - To ensure interoperability, the standards for each interface / service must be identified
  - For example: If a system will have SATCOM capability, SATCOM standard(s) must be defined
  - Systems will generally implement only a subset of the DISR standards

# DISRonline Website

- Replaces (includes) the former JTA website
  - http://disronline.disa.mil/
- DISRonline contains tools, questionnaires, user guides to create IT profiles
- DISRonline lists the standards included in each of the JTA / DISR versions
  - Standards are NOT available from DISRonline, however links to the standards organizations are provided

# Joint Tactical Radio System (JTRS)

# JTRS Overview

- JTRS is a family of software programmable radios
- Multichannel voice, data, imagery, and video communications. Networking services.
- Will be able to communicate (and will eventually replace) all legacy radios
  - Goal is to eliminate interoperability problems
  - Sea, land, air, and space
  - DoD and allies, possibly law enforcement and homeland security
- All new acquisitions or modifications must be JTRS compliant, unless a waiver is granted
- http://jtrs.army.mil